HACKING HACKING HACKING 101 HACKING HACKING HACKING

This article is the first in a series of articles that address the oft-asked question, "How do I become a hacker?"

"Footprinting" A System

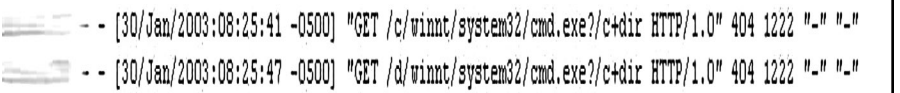
By: StankDawg

StankDawg@hotmail.com

Hacking is a very broad term that can refer to many things. In the context of this article, I am going to use hacking fundamentals to help you to "think outside the lines." It may sound cliché to say it, but once you get the hang of the concepts that I am teaching you, and the precise ways to accomplish each goal, you will start to understand the mindset of a hacker.

One of the things that most hackers have in common is the concept of thinking their way around things. When faced with a problem, or a situation that seems to have no options, hackers are able to make options appear. Before a hacker considers the situation closed, they make sure that all possibilities have been examined. This entails gathering all of the information about a given situation and thinking about where that information can lead them. With all of the information at hand, more options can be discovered. In a technical environment, this means "footprinting" a system to get all of the information you can about a particular environment in order to thoroughly investigate it.

Why is this step necessary? Many hackers don't know what it means to footprint a system and others simply do not see the value in it. By footprinting a system, you will get detailed information that will keep you from using inappropriate tools or methods of attack on a system. For example, in the screen shot below, you will notice that an attacker is trying to use a known exploit to break into my server. If this user had done a little bit of work beforehand and footprinted my system, they would have known that I am running an Apache web server on a machine using the Linux operating system. The exploit that they were trying to use only works in systems running specific versions of Microsoft Windows. This is obviously the work of a "script kiddie" who doesn't understand basic hacking concepts. This attacker was probably just going through a range of IP addresses using the same exploits, hoping that he gets lucky and finds one purely by accident. I wish him luck.



Screen Capture 1 - IP address blurred to protect the incompetent

To "footprint" a system, or to get a "footprint" of a system means to use logic and technological understanding to obtain all of the publicly available information about a system. Why is this important? Sun Tsu stated in his famous writing **The Art of War,** *"…that general is skillful in attack whose opponent does not know what to defend."*